

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2004-080663**

(43)Date of publication of application : **11.03.2004**

(51)Int.Cl.

H04L 9/08

(21)Application number : **2002-241447**

(71)Applicant : **ABEL SYSTEMS INC**

(22)Date of filing : **22.08.2002**

(72)Inventor : **SUZUKI FUMIO**

ITAYA SATOKO

SUZUKI AKO

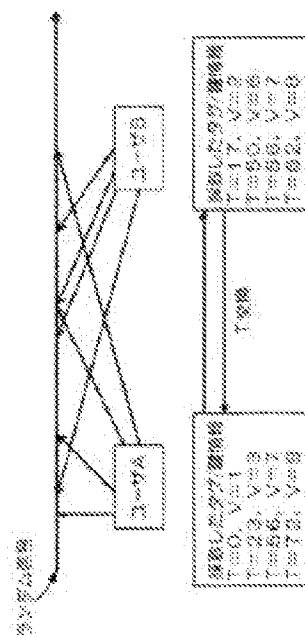
MIZUKAWA SHIGEMITSU

(54) METHOD, APPARATUS, AND PROGRAM FOR GENERATING ENCODING/DECODING KEY, AND COMPUTER READABLE RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method for safely acquiring an encoding key and a decoding key.

SOLUTION: The method for generating encoding/decoding key using a computer includes a step where first and second receiving parts sample random signal from a prescribed source by a prescribed method, a step where the random signal sampled by the first and second receiving parts is divided into tag information and key information, a step where the tag information acquired by the first and second receiving parts is exchanged with each other, a step where a common tag is extracted from the set of tag information exchanged between the first and second receiving parts, and a step where the first and second receiving parts generate keys for encoding and decoding using key information corresponding to the common tag.



(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-80663

(P2004-80663A)

(43) 公開日 平成16年3月11日(2004.3.11)

(51) Int.Cl.⁷

H04L 9/08

F 1

H04L 9/00

601C

テーマコード (参考)

5J104

H04L 9/00

601A

審査請求 未請求 請求項の数 16 O L (全 23 頁)

(21) 出願番号 特願2002-241447 (P2002-241447)
 (22) 出願日 平成14年8月22日 (2002.8.22)

(71) 出願人 500404258
 アーベル・システムズ株式会社
 京都府京都市西京区大枝北沓掛町二丁目3
 番地の16
 (74) 代理人 100104949
 弁理士 豊栖 康司
 (74) 代理人 100074354
 弁理士 豊栖 康弘
 (72) 発明者 鈴木 文雄
 京都府京都市西京区大枝北沓掛町二丁目3
 番地の16
 (72) 発明者 板谷 聡子
 大阪府箕面市如意谷4 6 17 201

最終頁に続く

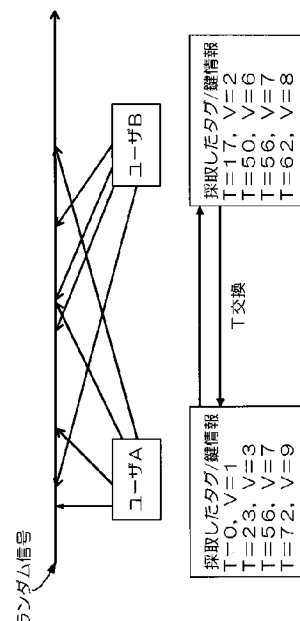
(54) 【発明の名称】 暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体

(57) 【要約】

【課題】 安全に暗号化鍵および復号鍵を取得する方法を提供する。

【解決手段】 電子計算機を使った暗号化／復号鍵の鍵生成方法は、第1および第2の受信部がそれぞれ所定のソースからランダム信号を所定の方法でサンプリングするステップと、第1および第2の受信部がそれぞれサンプリングしたランダム信号をタグ情報と鍵情報に分割するステップと、第1および第2の受信部がそれぞれ取得したタグ情報を相互に交換するステップと、第1および第2の受信部がそれぞれ交換されたタグ情報の集合から共通するタグを抽出するステップと、第1および第2の受信部がそれぞれ共通するタグと対応する鍵情報を使って暗号化および復号のための鍵を生成するステップとを有する。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

電子計算機を用いる暗号化もしくは復号のための鍵の生成方法であって、
第 1 および第 2 の受信部がそれぞれ所定のソースからランダム信号を所定の方法でサンプリングするステップと、
前記第 1 および第 2 の受信部がそれぞれサンプリングしたランダム信号をタグ情報と鍵情報に分割するステップと、
前記第 1 および第 2 の受信部がそれぞれ取得したタグ情報から生成されたタグを相互に交換するステップと、
前記第 1 および第 2 の受信部がそれぞれ交換されたタグ集合から共通するタグを抽出するステップと、
前記第 1 および第 2 の受信部がそれぞれ前記共通するタグと対応する鍵情報を使い所定の方法で鍵を生成するステップと、
を備える暗号化／復号鍵の鍵生成方法。 10

【請求項 2】

暗号化もしくは復号のための鍵生成方法において、
第 1 および第 2 の受信部がそれぞれ所定のソースからランダム信号をブロックとして所定の方法でサンプリングするステップと、
前記第 1 および第 2 の受信部がそれぞれサンプリングした前記ブロックの一部をタグ情報として抽出するステップと、
前記第 1 および第 2 の受信部がそれぞれ取得したタグ情報から生成されたタグを相互に交換するステップと、
前記第 1 および第 2 の受信部がそれぞれ交換されたタグ集合から共通するタグを抽出するステップと、
前記第 1 および第 2 の受信部がそれぞれ前記共通するタグと対応するブロックの一部または全体を鍵情報として、前記鍵情報を用いて所定の方法で鍵を生成するステップと、
を有することを特徴とする暗号化／復号鍵の鍵生成方法。 20

【請求項 3】

前記鍵生成方法はさらに、
前記第 1 および第 2 の受信部がタグ情報から生成されたタグで、共通に持つタグと対応する鍵情報を複数組み合わせるステップを有することを特徴とする請求項 1 または 2 記載の暗号化／復号鍵の鍵生成方法。 30

【請求項 4】

前記鍵生成方法はさらに、
前記第 1 および第 2 の受信部が共通のタグ情報から生成されたタグと対応する鍵情報に対して、共通部分の鍵情報の抽出を行いその結果を相互に交換するステップを有することを特徴とする請求項 1 から 3 のいずれかに記載の暗号化／復号鍵の鍵生成方法。

【請求項 5】

前記鍵生成方法はさらに、
前記第 1 および第 2 の受信部がそれぞれ共通のタグ情報から生成されたタグ以外のタグ、およびこれと対応する鍵情報を鍵生成に使用しないものと判定するステップを有することを特徴とする請求項 1 から 4 のいずれかに記載の暗号化／復号鍵の鍵生成方法。 40

【請求項 6】

前記鍵生成方法はさらに、
前記第 1 および第 2 の受信部がランダム信号のサンプリングを開始するに先立ち、第 1 の受信部が第 2 の受信部に鍵の取得開始を通知するステップを有することを特徴とする請求項 1 から 5 のいずれかに記載の暗号化／復号鍵の鍵生成方法。

【請求項 7】

前記第 1 および第 2 の受信部がランダム信号のサンプリングを予め設定された方法で行うことを特徴とする請求項 1 から 6 のいずれかに記載の暗号化／復号鍵の鍵生成方法。 50

【請求項 8】

前記第 1 の受信部、または第 2 受信部がサーバであることを特徴とする請求項 1 から 7 のいずれかに記載の暗号化／復号鍵の鍵生成方法。

【請求項 9】

前記第 1 および第 2 の受信部がソースからランダム信号をサンプリングするための伝送媒体と、相互にタグ情報から生成されたタグを交換するための伝送媒体が別個の伝送媒体であることを特徴とする請求項 1 から 8 のいずれかに記載の暗号化／復号鍵の鍵生成方法。

【請求項 10】

前記ランダム信号を発生させる回数が制限されていることを特徴とする請求項 1 から 9 のいずれかに記載の暗号化／復号鍵の鍵生成方法。

10

【請求項 11】

暗号化もしくは復号のための鍵生成装置において、

ランダム信号を発生させるソースからランダム信号を所定の方法でサンプリングし、サンプリング情報からタグ情報と鍵情報を取得するためのサンプリング手段と、

取得したタグ情報から生成されたタグを他の生成装置と相互に交換するためのタグ交換手段と、

前記タグ交換手段で交換されたタグ集合から他の生成装置との間で共通するタグを抽出するためのタグ選択手段と、

前記共通するタグと対応する鍵情報を使って所定の方法で鍵を生成する鍵生成手段と、を備えることを特徴とする暗号化／復号鍵の鍵生成装置。

20

【請求項 12】

前記サンプリング手段が、

受信されたランダム信号からこれを選択するランダム信号採取部と、

受信されたランダム信号をタグ情報と鍵情報に分割する分割部と、

分割されたタグ情報と鍵情報を格納するためのタグ／鍵情報格納メモリと、

ランダム信号を選択する動作を制御する制御部と、

を備えることを特徴とする請求項 11 記載の暗号化／復号鍵の鍵生成装置。

【請求項 13】

前記サンプリング手段が、

ランダム信号を受信するランダム信号受信部と、

前記ランダム信号受信部で受信されたランダム信号を所定の期間連続的に格納するランダム信号格納メモリと、

前記ランダム信号格納メモリに格納されたランダム信号を選択するランダム信号採取部と、

採取されたランダム信号をタグ情報と鍵情報に分割する分割部と、

分割されたタグ情報と鍵情報を格納するためのタグ／鍵情報格納メモリと、

ランダム信号を選択する動作を制御する制御部と、

を備えることを特徴とする請求項 11 または 12 記載の暗号化／復号鍵の鍵生成装置。

30

【請求項 14】

前記分割部が、

受信したランダム信号を信号の種類に応じて分割するためのスプリッタと、

前記スプリッタで分割された信号にフィルタリングするためのフィルタと、

前記フィルタを通じたアナログ信号をデジタル信号に変換する A/D 変換手段と、

を備えることを特徴とする請求項 11 から 13 のいずれか記載の暗号化／復号鍵の鍵生成装置。

40

【請求項 15】

暗号化もしくは復号のための鍵生成プログラムにおいて、コンピュータに

ランダム信号を発生させるソースからランダム信号を所定の方法でサンプリングする機能と、

サンプリングしたランダム信号からタグ情報と鍵情報を取得する機能と、

50

取得したタグ情報から生成されたタグを他の鍵生成プログラムと相互に交換するステップと、
交換されたタグ集合から他の鍵生成プログラムとの間で共通するタグを抽出するステップと、
前記共通するタグと対応する鍵情報を使って鍵を生成するステップと、
を実現させるための暗号化／復号鍵の鍵生成プログラム。

【請求項16】

請求項15記載の暗号化／復号鍵の鍵生成プログラムを記録したコンピュータで読取可能な記録媒体。

【発明の詳細な説明】

10

【0001】

【発明が属する技術分野】

本発明は、暗号化もしくは復号のために使用する鍵を安全に生成できる暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成システム、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体に関する。例えば、鍵の生成装置やプログラムを使った暗号化システムの使用方法、利用方法を提案する。

【0002】

【従来の技術】

近年のネットワーク技術の飛躍的な発達とインターネット接続の爆発的な普及により、電子データによる情報のやりとりが一般化している。電子データをネットワークを介してやりとりする機会が増大すると共に、送受信される電子データの漏洩、解読を防止するセキュリティ技術の重要性が高まっている。特に電子メールの送付や電子ファイルの交換、あるいは電子商取引における個人情報の暗号化などの局面においては、個人情報や金銭に関する情報など秘密情報の漏洩を防止するためのセキュリティが重要となる。

20

【0003】

一般に応用が容易なセキュリティ技術としては、データの暗号化が利用されている。暗号化の方式としては、暗号化と復号（暗号解読）に同一の鍵を用いる対称鍵暗号が利用されている。しかしながらこの方式ではひとたび鍵を盗まれると第三者が容易に解読でき、秘密情報が完全に筒抜けになってしまうという欠点があった。

【0004】

30

このため、暗号化と復号に別々の鍵を用いる安全性の高い暗号方式として、公開鍵暗号方式が開発、利用されている。公開鍵暗号方式では、送信者と受信者が個別の公開鍵と秘密鍵の対をそれぞれ持っている。公開鍵は公開されており、送信に先立って例えば両者の間で電子メールなどにより交換したり、公開ウェブサーバからダウンロードするなどして入手する。そして送信者は受信者の公開鍵で暗号化した情報を送信する。暗号化された情報を受信した受信者は、受信者が秘密に持っている秘密鍵を使ってこれを復号する。公開鍵暗号を採用する方法として、例えばPGP (Pretty Good Privacy) があり、1024ビットなどの高い堅牢性を誇り、フリーで利用できるバージョンが公開されていることなどから広く利用されている。さらにその他の方式としてはPKCS (Public Key Cryptography Standards) やSSL (Secure Socket Layer)、S/MIME (Secure/Multi-Purpose Internet Mail Extensions) などが利用されている。

40

【0005】

【発明が解決しようとする課題】

しかしながら、公開鍵暗号を含めたいずれの暗号化方式でも安全性が完全に保証されるものではない。暗号化された情報の解読は暗号化方式が高度になるほど、いかにすると鍵長のビット数が多くなるほど困難となる。しかしこれは暗号解読により時間がかかるだけのものではあって、絶対に解読できないというものではない。またユーザは、暗号化もしくは復号するための鍵を予め交換する必要があるため、鍵を傍受される（盗まれる）可能性が

50

あり、これを使って暗号を解読される危険が依然として存在している。例えば同一の鍵を何度も使用している場合、鍵を盗まれたりして鍵が第三者の手に渡る危険性がある。鍵と暗号化された情報が（暗号文）第三者の手に渡ると、第三者は容易に暗号文を解読できる。あるいは安全性の低い鍵を使用すると、いくつかの暗号文から鍵そのものを知られてしまうことにもなる。いうなれば、安全性の低い鍵で情報を暗号化したとしても、その暗号文は暗号知識を有する者にとって暗号化されていない（平文）秘密情報と同等である。

【0006】

本発明は、従来の暗号化技術が持つ根本的な問題、すなわち暗号化もしくは復号のための鍵の交換プロセスに注目し、この段階での鍵の漏洩を防止することを目的に開発されたものである。本発明の主な目的は、暗号化／復号鍵の鍵配信の際に第三者に傍受される事態を回避するシステムを提供し、鍵の漏洩を防止し暗号解読に対して安全性の高い暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成システム、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を提供することにある。

10

【0007】

【課題を解決するための手段】

上記課題を解決するための本発明の請求項1に記載される発明は、暗号化もしくは復号のための暗号化／復号鍵の鍵生成方法に関するものである。この鍵生成方法は、第1および第2の受信部がそれぞれ所定のソースからランダム信号を所定の方法でサンプリングするステップと、前記第1および第2の受信部がそれぞれサンプリングしたランダム信号をタグ情報と鍵情報に分割するステップと、前記第1および第2の受信部がそれぞれ取得したタグ情報から生成されたタグを相互に交換するステップと、前記第1および第2の受信部がそれぞれ交換されたタグ集合から共通するタグを抽出するステップと、前記第1および第2の受信部がそれぞれ前記共通するタグに対応する鍵情報を使って所定の方法で鍵を生成するステップとを有することを特徴とする。前記第1および第2の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

20

【0008】

また、本発明の請求項2に記載される暗号化／復号鍵の鍵生成方法は、第1および第2の受信部がそれぞれ所定のソースからランダム信号をブロックとして所定の方法でサンプリングするステップと、前記第1および第2の受信部がそれぞれサンプリングした前記ブロックの一部をタグ情報として抽出するステップと、前記第1および第2の受信部がそれぞれ取得したタグ情報から生成されたタグを相互に交換するステップと、前記第1および第2の受信部がそれぞれ交換されたタグ集合から共通するタグを抽出するステップと、前記第1および第2の受信部がそれぞれ前記共通するタグに対応するブロックの一部または全体を鍵情報として、前記鍵情報を用いて所定の方法で暗号化／復号鍵の鍵を生成するステップとを有することを特徴とする。前記第1および第2の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

30

【0009】

さらに、本発明の請求項3に記載される暗号化／復号鍵の鍵生成方法は、上記請求項1または2に記載される特徴に加えて、さらに前記第1および第2の受信部が共通するタグに対応する鍵情報を複数組み合わせ鍵を合成するステップを有することを特徴とする。前記第1および第2の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

40

【0010】

さらにまた、本発明の請求項4に記載される暗号化／復号鍵の鍵生成方法は、上記請求項1から3のいずれかに記載される特徴に加えて、さらに前記第1および第2の受信部がタグ情報から生成されたタグで、共通のタグに対応する鍵情報に対して、鍵情報の共通部分の抽出を行い、その結果を相互に交換するステップを有することを特徴とする。前記第1および第2の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

【0011】

さらにまた、本発明の請求項5に記載される暗号化／復号鍵の鍵生成方法は、上記請求項1から4のいずれかに記載される特徴に加えて、さらに前記第1および第2の受信部がそ

50

れぞれ共通するタグ情報から生成されたタグ以外のタグおよびこれと対応する鍵情報を鍵生成に使用しないものと判定するステップを有することを特徴とする。前記第1および第2の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

【0012】

さらにまた、本発明の請求項6に記載される暗号化／復号鍵の鍵生成方法は、上記請求項1から5のいずれかに記載される特徴に加えて、さらに前記第1および第2の受信部がランダム信号のサンプリングを開始するに先立ち、第1の受信部が第2の受信部に鍵の取得開始を通知するステップを有することを特徴とする。前記第1および第2の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

【0013】

さらにまた、本発明の請求項7に記載される暗号化／復号鍵の鍵生成方法は、上記請求項1から8のいずれかに記載される特徴に加えて、前記第1および第2の受信部がランダム信号のサンプリングを予め設定された方法で行うことを特徴とする。前記第1および第2の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

【0014】

さらにまた、本発明の請求項8に記載される暗号化／復号鍵の鍵生成方法は、上記請求項1から7のいずれかに記載される特徴に加えて、前記第1または第2の受信部がサーバであることを特徴とする。前記第1および第2の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

【0015】

さらにまた、本発明の請求項9に記載される暗号化／復号鍵の鍵生成方法は、上記請求項1から8のいずれかに記載される特徴に加えて、前記第1および第2の受信部がソースからランダム信号をサンプリングするための伝送媒体と、相互にタグ情報から生成されるタグを交換するための伝送媒体が別個の伝送媒体であることを特徴とする。前記第1および第2の受信部は各々別の装置としてもよいし、同一の装置としてもよい。

【0016】

さらにまた、本発明の請求項10に記載される暗号化／復号鍵の鍵生成方法は、上記請求項1から9のいずれかに記載される特徴に加えて、前記ランダム信号を発生させる回数が制限されていることを特徴とする。

【0017】

一方、本発明の請求項11に記載される発明は、暗号化もしくは復号のための鍵生成装置に関するものである。この鍵生成装置は、ランダム信号を発生させるソースからランダム信号を所定の方法でサンプリングし、サンプリング信号からタグ情報と鍵情報を取得するためのサンプリング手段と、取得したタグ情報から生成されたタグを他の生成装置と相互に交換するためのタグ交換手段と、前記タグ交換手段で交換されたタグ集合から他の生成装置との間で共通するタグを抽出するためのタグ選択手段と、前記共通するタグと対応する鍵情報を使って所定の方法で鍵を生成する鍵生成手段とを備えることを特徴とする。

【0018】

また、本発明の請求項12に記載される暗号化／復号鍵の鍵生成装置は、上記請求項11に記載される特徴に加えて、前記サンプリング手段が、受信されたランダム信号からこれを採取するランダム信号採取部と、受信されたランダム信号をタグ情報と鍵情報に分割する分割部と、分割されたタグ情報と鍵情報を格納するためのタグ／鍵情報格納メモリと、ランダム信号を採取する動作を制御する制御部とを備えることを特徴とする。

【0019】

さらにまた、本発明の請求項13に記載される暗号化／復号鍵の鍵生成装置は、上記請求項11または12に記載される特徴に加えて、前記サンプリング手段が、ランダム信号を受信するランダム信号受信部と、前記ランダム信号受信部で受信されたランダム信号を所定の期間連続的に格納するランダム信号格納メモリと、前記ランダム信号格納メモリに格納されたランダム信号を採取するランダム信号採取部と、採取されたランダム信号をタグ情報と鍵情報に分割する分割部と、分割されたタグ情報と鍵情報を格納するためのタグ／

10

20

30

40

50

鍵情報格納メモリと、ランダム信号を採取する動作を制御する制御部とを備えることを特徴とする。

【0020】

さらにまた、本発明の請求項14に記載される暗号化／復号鍵の鍵生成装置は、上記請求項11から13のいずれかに記載される特徴に加えて、前記分割部が、受信したランダム信号を信号の種類に応じて分割するためのスプリッタと、前記スプリッタで分割された信号にフィルタリングするためのフィルタと、前記フィルタを通じたアナログ信号をデジタル信号に変換するA/D変換手段とを備えることを特徴とする。

【0021】

また、本発明の請求項15に記載される発明は、暗号化もしくは復号のための鍵生成プログラムに関するものである。この暗号化／復号鍵の鍵生成プログラムは、コンピュータに、ランダム信号を発生させるソースからランダム信号を所定の方法でサンプリングする機能と、サンプリングしたランダム信号からタグ情報と鍵情報を取得する機能と、取得したタグを他の暗号鍵生成プログラムと相互に交換するステップと、交換されたタグ集合から他の鍵生成プログラムとの間で共通のタグ情報から生成されたタグを抽出するステップと、前記共通するタグと対応する鍵情報を使って鍵を生成するステップとを実現させるためのプログラムである。

【0022】

さらにまた、本発明の請求項16に記載されるコンピュータで読取可能な記録媒体は、上記請求項15に記載される前記暗号化／復号鍵の鍵生成プログラムを記録したものである。記録媒体には、CD-ROM、CD-R、CD-RWやフレキシブルディスク、磁気テープ、MO、MD、DVD-ROM、DVD-RAM、DVD-R、DVD+R、DVD-RW、DVD+RWなどの磁気ディスク、光ディスク、光磁気ディスク、半導体メモリその他のプログラムやデータなどを格納可能な媒体が含まれる。またプログラムがネットワークを介してダウンロード可能として配布する形態も包含する。

【0023】

従来の考え方では、どのようにして暗号化／復号鍵の鍵を解読され難くするかというアプローチで安全性を高める技術が開発されていた。これに対し本発明は、各ユーザがそれぞれ異なる位置、時間においてランダム信号をサンプリングし、これを利用して暗号化／復号鍵の鍵を生成するという別の観点から開発されたものである。特に鍵やその元となるデータ自体を交換しないことによって、例えば通信を傍受されたとしても鍵を入手、再現されることはない。鍵を生成するアルゴリズムは既存の方法が利用できるため、本発明を様々な暗号化システムに利用してより安全性の高いデータ交換や配信が実現される。

【0024】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。ただし、以下に示す実施の形態は、本発明の技術的思想を具体化するための暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成システム、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を例示するものであって、本発明は暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成システム、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を以下のものに特定しない。

【0025】

またこの明細書は、特許請求の範囲に示される部材を、実施の形態の部材に特定するものではない。なお、各図面が示す部材の大きさや位置関係などは、説明を明確にするため誇張していることがある。さらに、本発明を構成する各要素は、複数の要素を同一の部材で構成して一の部材で複数の要素を兼用する態様としてもよい。

【0026】

本明細書において電子計算機には、いわゆるコンピュータに限られず、システムLSIやCPU、MPUやその他のICを使用した装置、回路その他の組み込み機器や素子自体を包含する意味で使用する。

10

20

30

40

50

【0027】

本明細書において暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成システムおよび暗号化／復号鍵の鍵生成プログラムは、暗号化／復号鍵の鍵生成における鍵の生成や鍵の送信動作そのもの、ならびに生成された鍵の利用など暗号化／復号鍵の鍵生成に関連する入出力、表示、演算、通信その他の処理をハードウェア的に行う装置や方法に限定するものではない。ソフトウェア的に処理を実現する装置や方法も本発明の範囲内に包含する。例えば汎用の回路やコンピュータにソフトウェアやプログラム、プラグイン、オブジェクト、ライブラリ、アプレット、コンパイラ、モジュール、特定のプログラム上で動作するマクロなどを組み込んで鍵生成などを実施可能とした汎用あるいは専用のコンピュータ、ワークステーション、端末、携帯型電子機器、PDC、CDMA、GSM、IMT2000や第4世代などの携帯電話、PHS、PDA、ページャ、スマートフォンその他の電子デバイスも、本発明の暗号化／復号鍵の鍵生成方法および暗号化／復号鍵の鍵生成システムに含まれる。また本明細書においては、プログラム自体も暗号化／復号鍵の鍵生成システムに含むものとする。さらに本明細書においてプログラムとは、単体で使用されるものに限られず、特定のコンピュータプログラムやソフトウェア、サービスなどの一部として機能する態様や、必要時に呼び出されて機能する態様、OSなどの環境においてサービスとして提供される態様、環境に常駐して動作する態様、バックグラウンドで動作する態様やその他の支援プログラムという位置付けで使用することもできる。

10

【0028】

本発明の実施例において使用されるコンピュータなどの端末同士、およびサーバやこれらに接続される操作、制御、入出力、表示、各種処理その他のためのコンピュータ、あるいはプリンタなどその他の周辺機器との接続は、例えばIEEE1394、RS-232XやRS-422、USBなどのシリアル接続、パラレル接続、あるいは10BASE-T、100BASE-TX、1000BASE-Tなどのネットワークを介して電氣的に接続して通信を行う。接続は有線を使った物理的な接続に限られず、IEEE802.11Xなどの無線LANやBluetoothなどの電波、赤外線、光通信などを利用した無線接続などでもよい。さらにデータの交換や設定の保存などを行うための記録媒体には、メモ리카ードや磁気ディスク、光ディスク、光磁気ディスク、半導体メモリなどが利用できる。

20

【0029】

また本明細書においては、特に断りのない限り「暗号化」とはデータの暗号化と共に、暗号化されたデータの復号または暗号解読を含むものとする。

30

【0030】

上述のように、暗号化／復号鍵の鍵は傍受される危険が伴う。送信者と受信者間で鍵を交換する際、インターネットのようなオープンなネットワークを介して鍵が送信される以上、第三者の傍受の可能性は常にある。これを防止するために専用回線を介して鍵を交換したり、記録メディアに保存して物理的に交換するなどの手段もあるが、いずれも手間がかかる。これらの方法と比較すると、電子データによるネットワークを介した鍵の交換が最も簡単かつ迅速な手段であることは明らかである。よって、インターネットなどの高速に利用できるネットワーク回線を利用することを前提として、安全に鍵を生成する方法を確立することが情報通信技術において極めて重要となる。

40

【0031】

現在、安全性の高い鍵配信方法として、量子(Quantum: 1量子の動き)を利用した鍵配信方法が提案されている[C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, "Experimental Quantum Cryptography", Journal of Cryptology, Vol. 5, No. 3, 1992]。この方法では、配信された鍵を傍受している第三者が存在することを検知することができる。

【0032】

しかしながら、この方法を実現するには単一量子を扱うことのできる装置が必要で、単一

50

量子を扱うための特殊な装置は実施化が技術的に難しいという問題があった。量子を利用した技術には、例えば特開2001-7798号公報などがある。

【0038】

さらに、上記問題を解決する手段として、情報理論的に安全な方法が提案されている[C. Cachin and U. Maurer, "Unconditional Security Against Memory-Bounded Adversaries", Advances in Cryptology CRYPTO '97, B. Kaliski (Ed.), Lecture Notes in Computer Science, Vol. 1294, Springer-Verlag, 1997, pp. 292-306; Y. Aumann and M. O. Rabin, "Information Theoretically Secure Communication in the Limited Storage Space Model", Advances in Cryptology CRYPTO '99, M. J. Wiener (Ed.), Lecture Notes in Computer Science, Vol. 1666, Springer-Verlag, 1999, pp. 65-79]。この方法は、データの送信者と受信者が同一のソースから送出される乱数列をサンプリングして、これを鍵として使用する方法である。仮に、送信者と受信者がソースから送出される乱数列からデータを採取している時間内に、ソースから送信されるデータの数を N^P 、送信者と受信者が採取できるデータの数を N^S とする。ここで、サンプリング数が極めて多く、また、ソースから送出される乱数の量がサンプリング数より十分に多いと仮定すると、 $N^P \gg N^S \gg 1$ となる。このとき、受信者と送信者で、一回のサンプリング毎に一致しているデータの総数の期待値は $(N^S / N^P) \times N^S = N^{2S - P}$ である。

【0034】

この暗号化／復号鍵のサンプリングの際に、同一のソースから送出される乱数列を同様にサンプリングする第三者すなわち盗聴者が存在する場合を考える。同時に第三者が乱数列から採取できるデータ数も、送信者や受信者と同レベルと考えるのが一般的であるので、 N^S とする。このとき、送信者と受信者で一致した乱数データを第三者が共通して所有する一致しているデータの総数の期待値は $(N^{2S - P} / N^P) \times N^S = N^{3S - 2P}$ である。つまり、 N^S と N^P の値を適切に調整することにより、第三者が送信者・受信者と共通のデータを持つ期待値を限りなく0に近づけることができる。例えば、送信者Aと受信者Bのサンプルが一致する数の期待値を N_{AB} と、送信者Aと受信者Bと第三者Eのサンプルが一致する数の期待値を N_{ABE} となるようにするため、 $N^P = N_{AB}^3 / N_{ABE}^2$ 、 $N^S = N_{AB}^2 / N_{ABE}$ とすればよい。このシステムは、ソースから大量に純粋な乱数が発生されるのに対し、乱数を採取する側、すなわち送信者と受信者と第三者において、乱数採取を行うシステムが一部の数のサンプルしかできないことを前提としている。このシステムでは、従来のように暗号化／復号に同じ鍵を何度も用いることなく、特定の乱数を鍵として一回だけ暗号化／復号に用いるため、鍵を盗まれにくく秘匿性を高めることができる。

【0035】

しかしながら、上記の報告例は理論の提案に止まり、具体的に実施化するためのモデルが提示されていない。具体的には、ランダム信号からデータをどのようにして取り出し、また取り出したデータが共通のものであることをどのようにして認識するかといった点が明らかにされていない。

【0036】

そこで本発明者らは鋭意研究を重ねた結果、この提案を具体的に実現する方法を発明し、秘匿性の高い暗号化／復号鍵の鍵生成システムを開発するに至った。本システムでは、多変量ランダム信号、多変ビットランダム信号または複合ランダム信号からタグと鍵を取得する。このシステムでは、離れた者同士が鍵を交換することなくランダム信号を共有することができ、このランダム信号を鍵情報として利用する。このようにして取得した鍵は、

そのまま暗号化乱数としても利用できるし、またはより高度な暗号化の鍵やIDのようなものとしても用いることもできる。

【0037】

また様々な暗号やセキュリティシステムに実装して利用する形態も考えられる。応用分野の一例としては、モバイルシステム、ポイント・トゥ・ポイント（Point-to-Point）システムや無線LAN、UWBでイーサネット（登録商標）を用いたユーザ間のやり取りなどが挙げられる。

【0038】

以下、本発明の実施例を使って、ユーザAとユーザBが共通の鍵を入手する手法を説明する。共通の鍵を安全に取得したユーザAとユーザBは、この鍵を使って暗号化／復号を行い安全なやりとりを行うことができる。図1は本発明の1実施例に係る暗号化／復号鍵の鍵取得方法で各ユーザがランダム信号をサンプリングする様子を時系列的に示したものである。このシステムは、図2に示すように、ランダム信号を発生するソース1と、伝達媒体2とを備え、ランダム信号のソースとユーザAとユーザBが伝達媒体2に接続している。ユーザA、Bはそれぞれランダム信号のソース1からランダム信号列をサンプリングし、得られたランダム信号をそれぞれタグ情報Tと鍵情報Vに分割する。そしてタグ情報Tのみを相互に交換し、共通するタグ情報Tと対応する鍵情報Vのみを残しこれを用いて鍵を生成する。ここで図1のようなタグ情報T、鍵情報VをユーザA、Bがそれぞれ取得したとすれば、T=56と対応するV=7のみを残す。

10

【0039】

図2の例では、ソース1は純粋なランダム信号を連続的に発生させるランダム信号源である。ソース1はランダム信号を発生させるものであれば何でもよい。ソース1はランダム信号を伝達媒体2を介して送出する。伝達媒体2は、通信が可能な媒体であればよく、LAN、インターネット網や電話線などの公衆回線や専用回線が使用できる。接続方式や通信方式も限定されず、イーサネット（登録商標）、シリアル、パラレル、IEEE1394、USBなどが利用でき、媒体は銅線ケーブルや光ファイバーなど、通信に適したものであればよい。また物理的な媒体を使って電気信号を伝達する手段に限られず、電波、無線LAN、Bluetoothなど無線による通信や赤外線通信、光通信など、信号をやりとりできるあらゆる手段を含む。

20

【0040】

また図2の例では、伝達媒体がランダム信号を送出するランダム信号線と、後述するようにユーザAとユーザBがタグ情報を交換、比較するためのタグ情報通信線を兼ねている。ただ、図3に示すようにランダム信号線2aとタグ情報通信線2bを個別に設けてもよい。この場合は複数の回線もしくはチャンネルを使用してデータのやりとりをするため、通信傍受がより困難になるというメリットがある。例えば、ランダム信号線をインターネット回線とし、タグ情報通信線を電話回線とする。もちろん、有線通信と無線通信を混在させることも可能であることは言うまでもない。

30

【0041】

ユーザAとユーザBは、伝達媒体2を介してランダム信号のソース1から送信されるランダム信号を採取することができる。各ユーザは、ランダム信号をサンプリングするサンプリング手段3を備える。サンプリング手段3の一例を図4および図5に示す。図4に示すサンプリング手段3は、ランダム信号受信部8と、ランダム信号採取部4と、分割部5と、タグ／鍵情報格納メモリ6と、制御部7を備える。このサンプリング手段3はシステムLSIなどで構成できる。また、ランダム信号受信部8は、サンプリング手段3と外部で接続されてもよい。ランダム信号受信部8は所定の方法あるいはタイミングで、ランダム信号のソース1からランダム信号を連続的に取得する。取得するランダム信号はブロックまたは波形パターンとしてランダム信号採取部4で採取され、分割部5に送出する。分割部5は、採取したランダム信号をタグ情報Tと鍵情報Vに分割し、分割された各タグ／鍵情報をタグ／鍵情報格納メモリ6に格納する。図12にブロック状のランダム信号列をタグ情報と鍵情報に分割する様子を示す。同じタグ情報が二度と現れない確率を十分小さく

40

50

するためには、タグ情報部分がある程度の長さを備えることが好ましい。以上の動作によってユーザはタグ情報Tと鍵情報Vを得ることができる。ランダム信号を採取する動作は、制御部7により制御される。制御部7は、制御変数としてサンプリングレート、シーケンス、ゲートなどを有している。

【0042】

ここで分割部の一例を図6に示す。この図に示す分割部は、スプリッタ9と、フィルタ10と、A/D変換手段11を備える。分割部は受信したランダム信号をスプリッタ9で信号の種類に応じて分割し、フィルタ10を通じてA/D変換手段11に送られる。フィルタ10は波長フィルタ、周波数フィルタ、時間遅延などが使用され、フィルタ10を通じたアナログ信号をA/D変換手段11によりデジタル信号に変換する。このようにして採取したランダム信号を二つのランダム信号に分割した後、デジタル信号に変換し、デジタル情報としてタグ情報Tと鍵情報Vに分割し、タグ/鍵情報格納メモリ6に格納する。

10

【0043】

一方、図5に示すサンプリング手段8は、ランダム信号受信部8Bと、ランダム信号格納メモリ12と、ランダム信号採取部13と、タグ/鍵情報格納メモリ6Bと、分割部5Bと、制御部7Bを備える。また、ランダム信号受信部8Bは、サンプリング手段8と外部で接続されてもよい。このサンプリング手段8も、システムLSIなどで構成できる。サンプリング手段8は、ランダム信号受信部8Bでランダム信号を受信し、ランダム信号格納メモリ12に所定の期間連続的に格納する。ランダム信号格納メモリ12は、レジスタなどで構成できる。ランダム信号格納メモリ12に格納されたランダム信号から、ランダム信号採取部13がランダム信号として採取し、分割部5Bに送る。分割部5Bは上記図4と同様、受信したランダム信号をタグTと鍵Vに分割し、分割された各情報をタグ/鍵情報格納メモリ6Bに格納する。これによってユーザはランダム信号としてタグTと鍵Vを得ることができる。ランダム信号を採取する動作は、上記と図4と同様に制御部7Bにより制御される。制御部7Bは、制御変数としてサンプリングレート、シーケンス、ゲートなどを有している。

20

【0044】

以上のサンプリング手段8を使って、各ユーザは所定のタイミングで、ソース1から送られるランダム信号のサンプリングを開始する。そしてサンプリングした情報をタグTと鍵に分割する。ここでサンプリングとは、所定のタイミングでソース1より送られてくるランダムな信号を、所定の方法で測定することを指すものとする。ランダム信号のサンプリングにより最終的にタグTと鍵Vを得る手法としては、図7、図8などの方法が利用できる。

30

【0045】

図7に示すサンプリング方法は、サンプリングを行うタイミングをタイミング信号生成部14で決定する。この方法では、タイミング信号生成部14でタイミング信号を発生するタイミングで、ランダム信号をランダム信号受信部8Cによりサンプリングし、A/D変換手段11CでA/D変換した後分割部5CでタグTと鍵Vに分割する。

【0046】

また図8に示す方法は、上記の方法のようにサンプリングした値をA/D変換した後にタグ情報と鍵情報に分割するのではなく、先にランダム信号をアナログ信号のまま分割部5Eでタグ信号と鍵信号とに分割しておき、分割されたタグ信号および鍵信号をそれぞれランダム信号受信部8EでサンプリングしてA/D変換手段11EでA/D変換し、タグTと鍵Vをそれぞれ得るものである。図8(a)に示す方法によって得られるタグ信号、鍵信号、タイミング信号の波形を図9に、また図8(b)に示す方法によって得られる各波形を図10に、それぞれ示す。これらの方法では、ランダム信号を図9(a)に示すチャンネル1のタグ信号と、図9(b)に示すチャンネル2の鍵信号に分割している。そしてタイミング信号生成部14Eで生成された図9(c)に示すタイミング信号のパルスがトリガとなって、この時点での値がそれぞれサンプリングされる。

40

【0047】

50

なお信号を分割する方法は様々な手法が利用でき、例えばランダム信号を2つに分割する、異なる波長で分割するなどが挙げられる。あるいは分割でなく、相関のない2つのランダム信号を用意して、特定の時間における信号をそれぞれタグ信号、鍵信号とすることもできる。例えば図10に示すようにチャンネル1とチャンネル2の2つのランダム信号のソース1A、1Bを用意し、一方をタグ信号のサンプリング用、他方を鍵信号のサンプリング用として利用する。この例では、図10(c)のような所定の信号をトリガ信号として、図10(d)のタイミング信号を発生する。図10(c)の信号が所定の値を超える、または所定のパターンが検出されたときをトリガとして、図10(a)、(b)に示すように、トリガ時のランダム信号の値をそれぞれタグ信号、鍵信号としてサンプリングする。

10

【0048】

さらに3つ以上のランダム信号を用いて、複数のランダム信号を組み合わせるなどの処理を加えることで新たなランダム信号を生成し、これをタグ信号や鍵信号とする、あるいはタグ信号と鍵信号に分割することもできる。

【0049】

以上のようにして、サンプリング手段8によりサンプリングしたデータからタグTと鍵Vを得ている。タグTは送信者と受信者間で交換するもので、鍵Vは実際に使用する鍵となる。ただ、タグと鍵を決定する手法はこれ以外にも採用でき、例えばサンプリングした全体のランダム信号を鍵情報とし、ランダム信号の一部をタグ情報として用いてもよい。

20

【0050】

〔実施例1〕

実施例1として、ユーザAとユーザB間の1:1の通信を考える。この場合、図11に示すフローチャートのような処理を行って暗号化/復号鍵の鍵を生成することができる。

【0051】

まずステップS1でユーザA、ユーザBはそれぞれランダム信号のソース1からサンプリングを開始する。サンプリングの開始は、各ユーザA、ユーザB間でサンプリングを開始する旨を何らかの手段で通知することもできるが、予め定められた所定の時間あるいは周期でそれぞれ開始してもよい。サンプリング動作は各ユーザA、ユーザBが同期を取ることなく任意に行う。所定の回数または時間のサンプリングが終了すると、ステップS2に進む。

30

【0052】

ステップS2では、お互いが取得したランダム信号の集合からタグ情報を交換する。タグ情報は各ユーザA、ユーザBがそれぞれ取得したランダム信号から抽出し、複数の時間におけるそれぞれのタグ情報を送付する。次にステップS3に進む。

【0053】

ステップS3では、交換したタグの内から共通するタグ情報を所定数含んでいるかどうかを確認する。共通するタグ情報が含まれていない場合、あるいは所定数の共通タグ情報に達していないときは、ステップS1に戻って再度サンプリングを行う。このとき、すでに取得したタグ情報および対応する鍵情報は鍵生成に使用しないものと判定し、破棄してもよいし、共通タグ情報と対応する鍵情報のみを保持していてもよい。共通するタグ情報が所定数含まれている場合は終了する。

40

【0054】

ステップS3の処理の後、共通するタグ情報に対応する鍵情報が正当であるかどうかのチェックを行うこともできる。ユーザAとユーザBがそれぞれの鍵情報に基づいて所定のビット列を計算し、タグ情報と共に相互に交換する。例えばハッシュ関数を用いて[Ti, H(Vi)]を交換する。これによって、タグ情報部分が一致しているにも拘わらず、鍵情報が異なるようなランダム信号を排除したり、エラーチェックを行うことができる。

【0055】

また、ステップS3の処理の後、暗号化/復号鍵の鍵生成を行うこともできる。鍵生成方法は、複数の鍵情報を組み合わせて行うこともできる。安全性を高めるために複数のタグ

50

情報および鍵情報を組み合わせる様子を図13に示す。図13では4ビットのタグ情報または鍵情報を複数列組み合わせ、4mビットのタグ、鍵をそれぞれ得ている。暗号化／復号鍵の鍵生成には、既知のプロトコルが使用できる。このようにして暗号化／復号鍵の鍵が生成されたことをユーザ同士で通知する。このときユーザ間で互いに送信、チェックを行ってもよいし、ユーザAがタグ情報やビット列をユーザBに送信し、ユーザB側のみでチェックを行ってもよい。

【0056】

〔実施例2〕

次に、ユーザが複数存在する場合にこれらのユーザ間で暗号化／復号鍵の鍵を生成する例について説明する。複数ユーザ間の通信では、図14のように1:nで各々が通信する場合と、図15のように特定のサーバを介して通信を行う場合が考えられる。まず、図14のようにユーザA、ユーザB、ユーザCの三者間でやりとりする実施例2の場合について説明する。基本的な手順は上述の実施例1と同様の手順となる。この場合ステップ2においては、ユーザA、ユーザB、ユーザCはそれぞれ自分以外の相手とタグ情報のやり取りをし、3者間で共通のタグ情報を共通タグとして保持する。複数のユーザが共通のタグを取得できる期待値は、ユーザ数nが大きくなるにつれ小さくなる。

10

【0057】

〔実施例3〕

さらに、図15に示すように複数のユーザ（ユーザ1、2、・・・、n）が特定のサーバを介して通信を行う例を実施例3として説明する。この図においてはユーザ間に位置するサーバと、クライアントに相当する各ユーザとの間でそれぞれ通信を行う形態となる。ユーザは他のユーザとの通信を行う際、直接ユーザ間で通信するのではなく一旦サーバを介して行うこととなる。この形態ではサーバと各ユーザとの間は1:1の通信となるため、基本的には実施例1と同様の手順で暗号化／復号鍵の鍵を生成する。その際、実施例2と異なり共通のタグを取得できる期待値はユーザ数に拘わらず一定となる。なお、ここでサーバとは分散処理システムにおいて他のユーザからの要求に応じて暗号化に関するサービスを提供するものの意味であって、例えば特定のユーザにこの役割をさせることもできる。

20

【0058】

さらにこの形態では、図16に示すようにタグテーブルを用意して各ユーザ間の通信で通信相手に対する暗号化／復号鍵の鍵をそれぞれ特定し、安全性を保持することができる。図16の例では、ユーザ1とユーザ2との間でタグテーブルを図のように設定している。例えば、サーバがユーザ1と通信する場合はタグT=3を共通タグとして採用し、サーバとユーザ2が通信する場合はタグT=8を使用する。また、ユーザ1とユーザ2が通信する場合、サーバはユーザ1とユーザ2で共通するタグとしてT=2を使用する。このようにして、ローカルなユーザ間の通信はサーバへ共通タグ情報を問い合わせ、対応する鍵情報により、ユーザ間でサーバを介して通信することができる。このため、すべてのユーザが相互にタグ情報の交換を行う必要はなく、サーバと各ユーザ間のやり取りだけでデータ通信を行うことができる。さらに、サーバから特定のユーザや複数のユーザで構成されたグループに対して、暗号化された情報を送信する際に、共通な鍵情報を得ることにより一度の暗号化で送信することができる。このとき、特定のユーザやグループ以外では共通ではない鍵を用いて暗号化されたデータであるため、サーバと通信しているすべてのユーザに向けて送信されたとしても、他のユーザは正当な鍵を持っていないのでこの情報を復号することができない。これによって、各ユーザへのデータ配信の際にも、通信相手以外のユーザに対しては情報の漏洩が防止され高い秘匿性が維持される。

30

40

【0059】

〔実施例4〕

さらにまた、サーバ・クライアント型のローカルな接続形態は、図17のようなネットワーク同士の接続にも応用することができる。この場合も実施例3、4と同様のシステムを導入して秘匿性を図ることができる。

【0060】

50

以上のシステムでは、タグ情報および鍵情報の元となる全てのランダム信号を、第三者が受信できないことが前提となる。有限の時間内のサンプリングといった、ランダム信号から限られた範囲のサンプリングのみが可能なシステムにおいて、送信者および受信者がタグ情報を交換することによって共通の鍵情報を見出すものである。したがって、システムのセキュリティを向上させるという面からは、ランダム信号の発生量が受信者あるいは第三者のランダム信号取得能力よりも大きい程セキュリティが高いことになる。

【0061】

さらに傍受の危険を回避するため、ランダム信号の発行回数を制限することとも可能である。ユーザが共通のランダム信号を受信すると、それ以上はランダム信号を発行しないように設定すれば、第三者がこれらのユーザと共通のランダム信号を取得することができなくなる。例えば、2者間の通信においてランダム信号を2回以上発行しないシステムとする。これによれば、情報の交換を行うユーザがそれぞれランダム信号を取得しようとしてランダム信号発生源にアクセスすると、ランダム信号発生源はランダム信号を発行するが、その発行回数を2回までに制限するのである。そうすると、ユーザが共通のランダム信号を受信すると、それ以上は同じランダム信号が発行されないの、仮に第三者が同じランダム信号にアクセスしようとしても、既に2回発行されたランダム信号を取得することはできない。このように、ランダム信号の発行回数を制限することによって、第三者によって同じランダム信号が傍受される危険を回避することができる。この方法は、例えば図15のようにサーバを介するシステムに利用すれば特定の2者間の通信に限られず、サーバを介して複数のクライアント間での通信が可能となる。また、このようなランダム信号の発行回数の制限には、ランダム信号発生源がランダム信号を発行する毎にフラグを設定し、フラグが2つまでランダム信号を発行できるように制限する方法などが利用できる。さらにサーバがランダム信号発生源をコントロールしてもよい。

【0062】

〔暗号化方式への実装〕

以上のようにしてランダム信号から共通に取得された鍵情報は、暗号化／復号のための鍵情報として用いることができ、ユーザ間で鍵そのものを交換することなく、従来の方式よりもより安全な暗号化／復号の鍵更新が実現する。また取得された鍵情報は鍵生成に使用するばかりでなく、暗号化のための乱数としても用いることができ、さらにその暗号化のための乱数を生成する種、例えば擬似乱数生成器の初期値としても用いることができる。そのほか複数個の鍵情報を合成して新たな鍵情報を生成することもできる。

【0063】

従来、暗号化／復号鍵の鍵を更新するには鍵そのものを何らかの方法でユーザ間で交換、あるいはサーバから配信、あるいは通信を行わない物理的な手段で更新する必要がある。インターネットなどオープンなネットワークを介して配信すると、漏洩の危険に晒されるため、公開鍵暗号などを利用した鍵配信方法を用いてユーザ間で交換、あるいはサーバから配信せざるを得ない。また、通信を行わない物理的な手段、例えば、フレキシブルディスクや磁気テープなどの記録媒体にデータを記憶して交換する方法が採られている。あるいはより高度な方法として、例えばネットワークにログインするパスワードを生成するために乱数を利用する方法が利用されている。この方法では、乱数発生器を内蔵し、乱数を表示可能なスマートカードやICカードを用意し、これをサーバに挿入するなどして物理的に接続する。これによってカードはサーバから乱数発生器の種を受ける。カードはユーザに物理的に配布される。乱数発生器は所定の周期で乱数を発生させるので、ユーザはログインする時点で表示されている乱数をパスワードとして利用する。この方法では定期的にパスワードとなる乱数が更新されるため、より高い安全性が確保される。

【0064】

しかしながら、いずれの方法も記録媒体やカードを使用して物理的に配布する工程が必要となり、このことが手間となっていた。これに対し本発明を利用すれば、従来不可能であった乱数の種をリモートで更新することが可能であり、物理的に鍵自体を交換するというリスクも冒すことなく安全に鍵を更新することが可能となる。また得られた暗号化および

復号のための鍵の使用は、一回切りとする使い捨て方式 (One-time Pad) とすれば、より安全性を高めることもできる。もちろん、鍵を複数回使用する形態にも利用できることはいうまでもない。

【0065】

以下、様々な暗号化方式に本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を応用した例について説明する。

【0066】

〔ストリーム（バーナム）暗号化方式〕

ストリーム暗号化方式では鍵系列（乱数系列）を用意し、暗号化に際して、平文系列の n ビット目と鍵系列の n ビット目の排他的論理和を取り、これを暗号文系列とする。一方、復号に際しては、暗号化と同じ鍵系列と同様の処理を行うことにより、平文系列を取り出す。本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を用いることにより、ストリーム暗号化方式に用いる鍵系列を生成するための初期値を、第三者に知られることなく保持することができる。また、最終的に排他的論理和をとるための鍵系列として本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を利用することもできる。以下、ストリーム暗号化方式を利用した例として、乱数生成部分にカオスを利用した G C C 暗号化方式および H D C P 暗号化方式に本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を実装した例を説明する。

【0067】

〔G C C 暗号化方式〕

ストリーム暗号化方式では、その安全性は主としてこの鍵系列として用いる乱数系列の性質に依存する。そこで、各種解読方法に対する強さが期待されているのがカオスの初期値に対する敏感な依存性を利用したカオス暗号化方式である。カオス暗号化方式は、例えば特開平 07-384081 号公報、米国特許第 5696826 号公報などに記載される。

【0068】

G C C 暗号化方式は、ストリーム暗号化方式の乱数生成部にカオス信号発生器を利用した暗号化方式である。このカオス信号発生器は複数のカオス発生関数からなる。入力された鍵に演算を施すことにより、使用するカオス発生関数番号、パラメータ、初期値を決定し、その値を用いてカオス信号を発生する。このカオス信号系列と平文系列の排他的論理和演算を取ることで、これを暗号文系列とする。ここで本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を利用すると、G C C 暗号化方式に用いる鍵を第三者に知られることなく更新または生成することができる。

【0069】

〔H D C P 暗号化方式〕

H D C P (High-bandwidth Digital Content Protection System) 暗号化方式は、デジタル・ビジュアル・インターフェース (Digital Visual Interface) からの出力を保護するために、インテル社が提案し、既に製品化されている技術である。このシステムでは、暗号化のための H D C P サイファ（H D C P Cipher）モジュールを持つ。このモジュールでは、線形フィードバックレジスタに蓄えたデータを入れ替え規則に従ってすることにより 24 ビットの擬似乱数データを生成する。この入れ替え操作に秘密デバイス鍵が用いられる。このシステムに本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を利用すると、H D C P 暗号化方式で使用される線形フィードバックレジスタに与える初期値、または H D C P 機器が必要とする秘密デバイス鍵の更新に応用することができる。

【0070】

このように、ストリーム暗号化方式に本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を利用すると、図18に示すように鍵系列（乱数系列）を生成するための種として、または安全な鍵生成および鍵更新を行うことができる。また、暗号化のための乱数系列として本発明で生成されるランダム信号を用いることができることはいうまでもない。さらにまた、AGCPなどデジタル画像配信のスクランブル用、またはストリーム暗号化方式のLFSRやOFBモード、CFBモードにも本発明を応用することができる。

【0071】

〔ブロック暗号化方式〕

次にブロック暗号化方式への実装について、図19に基づいて説明する。一般にブロック暗号化方式では、Festelの開発した暗号で用いられたいンボリューション（involution）と呼ばれる1:1変換ランダム処理テクニックが用いられる。その操作内容を決定するためには、暗号化／復号鍵の鍵、または鍵から導出される複数のサブ鍵が用いられる。ここで本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体により得られた鍵を、ブロック暗号化方式の暗号化／復号鍵、または複数のサブ鍵として用いることができる。

以下、ブロック暗号化方式を利用した例として、DES暗号とCAST暗号に、本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を実装した例を説明する。

【0072】

〔DES暗号化方式〕

DES（Data Encryption Standard）暗号化方式は、現在世界中で最も広く使われている暗号化方式である。DES暗号化方式は16段の変換部からなり、各段に用いるサブ鍵の生成は、ユーザから取得したパリティビットを含む64ビット鍵に対して複雑な処理を加えることで行われる。本発明は、DES暗号化方式のための64ビット秘密鍵や、その鍵から生成されるサブ鍵として用いることができる。本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を利用すると、DES暗号化方式の鍵として用いることができる。

【0073】

〔CAST暗号化方式〕

CAST暗号化方式は、エントラスト・テクノロジーズ（Entrust Technologies）が開発した暗号化方式である。各段階の換字、転置関数および鍵スケジューリング処理を工夫することで、DES暗号化方式よりも効果的に設計されている。本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体は、CAST暗号化方式の暗号化および復号の鍵を取得するために用いることができる。以上のように、本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体をブロック暗号に利用すると、ブロック暗号化方式の鍵を安全に取得できる。

【0074】

【発明の効果】

以上説明したように、本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体を利用すると、安全に暗号化／復号の鍵を生成することができる。それは、本発明の暗号化／復号鍵の鍵生成方法、暗号化／復号鍵の鍵生成装置、暗号化／復号鍵の鍵生成プログラムならびにコンピュータで読取可能な記録媒体が、鍵そのものをユーザ間で交換することなく、鍵情報と対応するタグ情報を使ってやりとりを行うからである。しかもタグ情報や鍵

情報はランダムに、ランダム信号のソースから採取するため再現性がない。また各ユーザはどのランダム信号が鍵情報として使用するか、採取する時点で決定することは不可能である。鍵情報の決定は、共通するタグ情報を抽出した以降となる。第三者においては、仮に交換されるタグ情報を傍受したとしても、タグに対応する鍵情報を事前に獲得していなければ、正当な鍵を得ることができない。また鍵情報は再現性のないランダム信号から採取されるため事後的に鍵情報を再現することはできない。鍵情報を得られない限り、復号あるいは暗号解読は計算理論上、鍵情報を得た時よりもはるかに困難となる。このように、本発明を既存の暗号化システムに利用することで第三者に暗号化／復号鍵を傍受される事態を回避して、安全性の高いデータのやりとりを実現することができるのである。

【図面の簡単な説明】

10

【図1】本発明の一実施例に係る暗号化／復号鍵の取得方法によりランダム信号をサンプリングする様子を時系列的に示した模式図である。

【図2】本発明の一実施例に係る暗号化／復号鍵の取得方法を構成する概略図である。

【図3】本発明の他の実施例に係る暗号化／復号鍵の取得方法を構成する概略図である。

【図4】ランダム信号をサンプリングするサンプリング手段の一例を示すブロック図である。

【図5】ランダム信号をサンプリングするサンプリング手段の他の例を示すブロック図である。

【図6】分割部の一例を示すブロック図である。

【図7】ランダム信号のサンプリング構成の一例を示すブロック図である。

20

【図8】さらにランダム信号のサンプリング構成の他の例を示すブロック図である。

【図9】図8(a)に示すサンプリング構成でサンプリングを行うタイミングを示すチャートである。

【図10】図8(b)に示すサンプリング構成でサンプリングを行うタイミングを示すチャートである。

【図11】ランダム信号をサンプリングして暗号化／復号鍵を生成する工程を示すフローチャートである。

【図12】ブロックのランダム信号をタグ情報と鍵情報に分割する様子を示す概念図である。

【図13】複数のタグ情報から鍵情報を組み合わせて、暗号化および復号のための鍵を構成する様子を示す概念図である。

30

【図14】複数のユーザ間で暗号化／復号鍵を生成する構成を示す概念図である。

【図15】複数のユーザ間でサーバを介して暗号化／復号鍵を生成する構成を示す概念図である。

【図16】タグテーブルに基づいて複数のユーザ間で暗号化／復号鍵を決定する様子を示す概念図である。

【図17】図15の接続形態を複数のネットワーク間に拡張した様子を示す概念図である。

【図18】本発明の実施例をストリーム暗号化方式に適用して鍵系列を生成する様子を示すブロック図である。

40

【図19】本発明の実施例をブロック暗号に適用した構成を示すブロック図である。

【符号の説明】

1、1A、1B・・・ランダム信号のソース

2・・・伝達媒体

2a・・・ランダム信号線

2b・・・タグ情報通信線

3・・・サンプリング手段

4・・・ランダム信号採取部

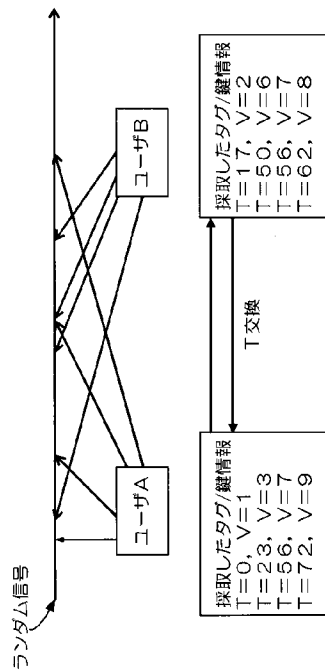
5、5B、5C、5D、5E・・・分割部

6、6B・・・タグ／鍵情報格納メモリ

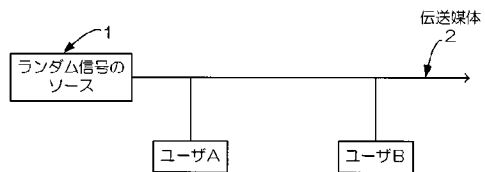
50

- 7、7 B・・・制御部
 8、8 B、8 C、8 E・・・ランダム信号受信部
 9・・・スプリッタ
 10・・・フィルタ
 11、11 C、11 D、11 E・・・A/D変換手段
 12・・・ランダム信号格納メモリ
 13・・・ランダム信号採取部
 14、14 E・・・タイミング信号生成部

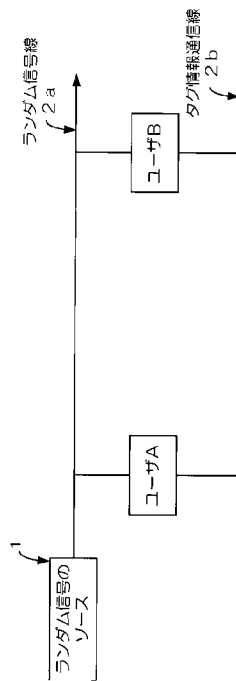
【図 1】



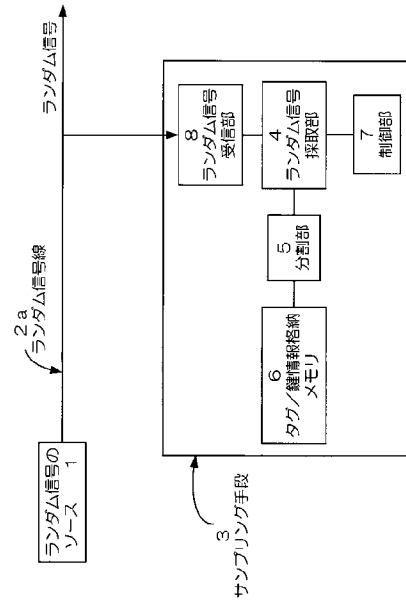
【図 2】



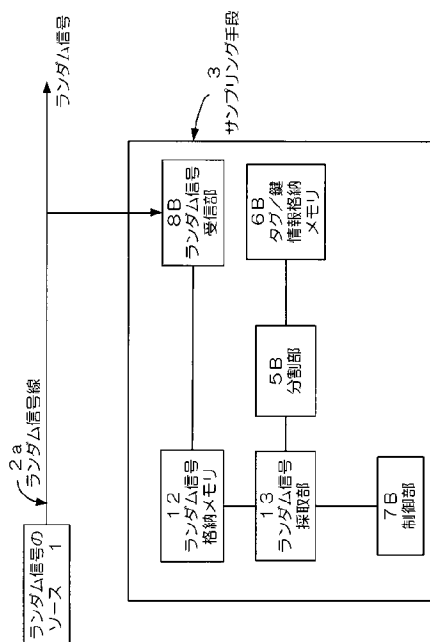
【図 3】



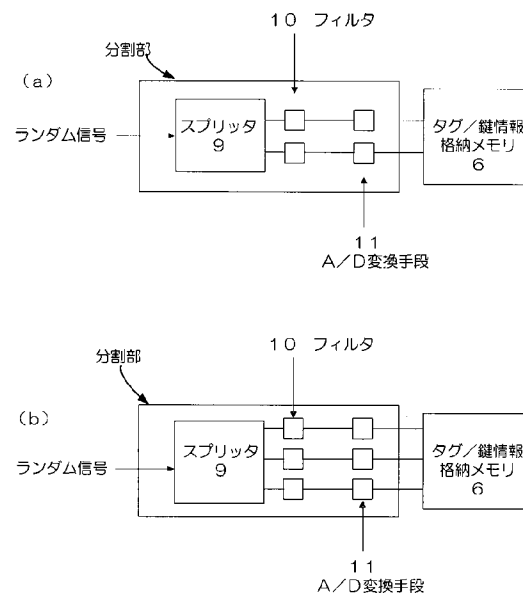
【図 4】



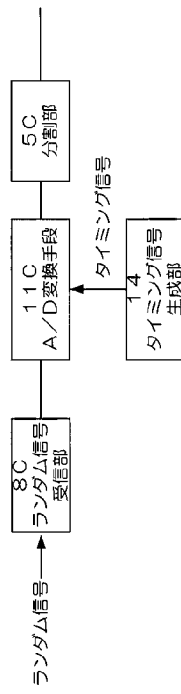
【図 5】



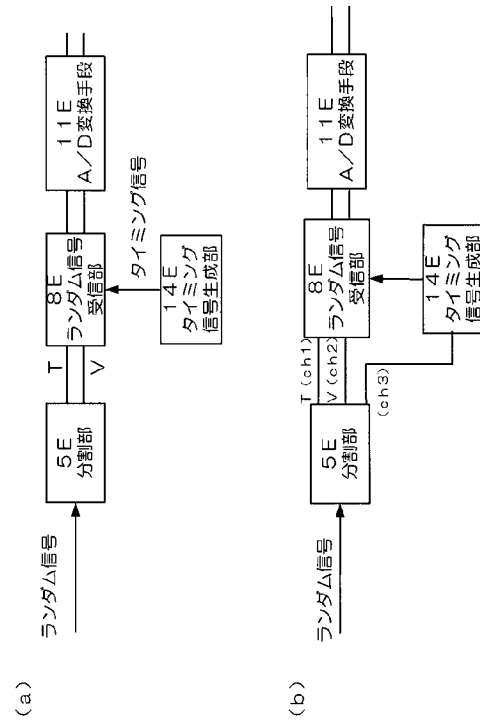
【図 6】



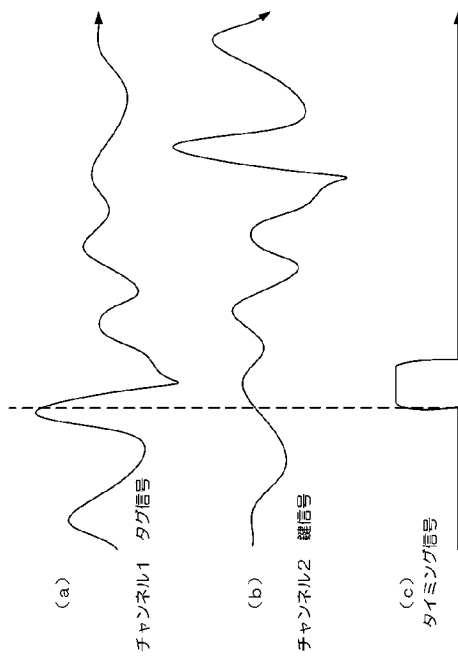
【図 7】



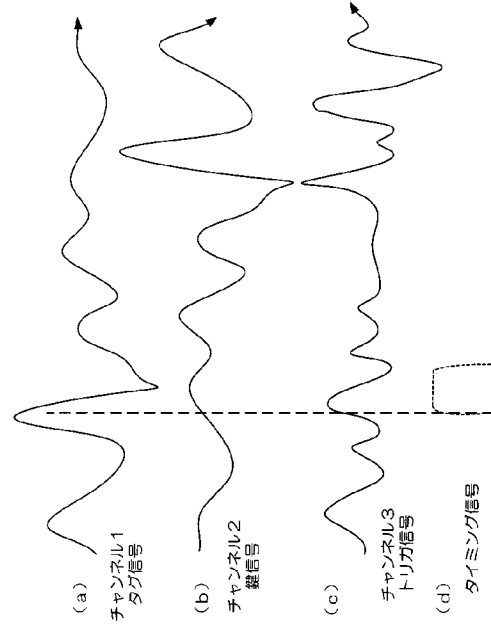
【図 8】



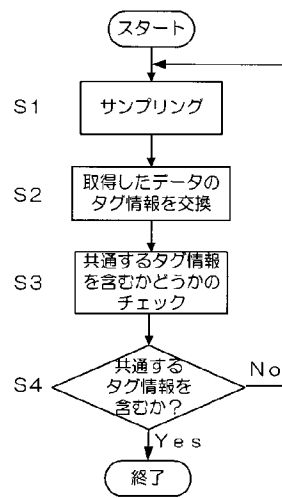
【図 9】



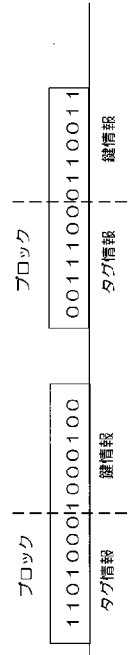
【図 10】



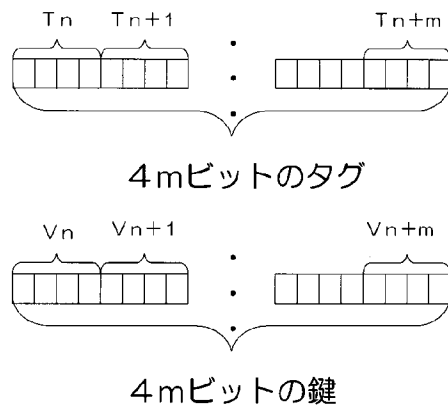
【図 1 1】



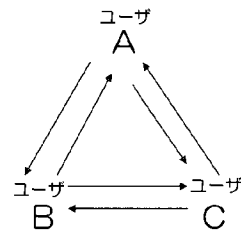
【図 1 2】



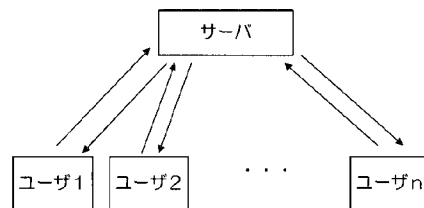
【図 1 3】



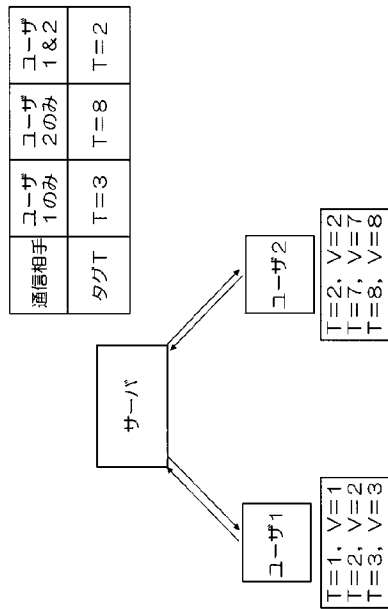
【図 1 4】



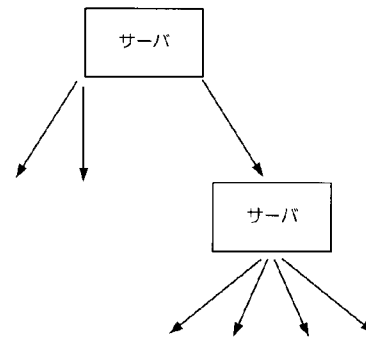
【図 1 5】



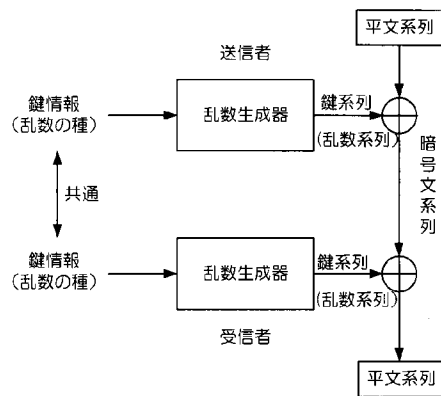
【図 16】



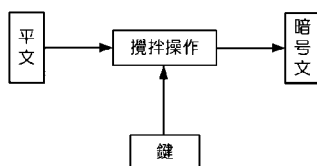
【図 17】



【図 18】



【図 19】



フロントページの続き

(72)発明者 鈴木 亞香

京都府京都市西京区大枝北沓掛町二丁目3番地の16

(72)発明者 水川 繁光

兵庫県宝塚市小浜5丁目1-1

Fターム(参考) 5J104 AA16 EA04 EA08 EA15 NA02